



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/531,491	11/14/2005	Heikki Waris	858.0001.U1(US)	9069
29683 7590 12/08/2009 HARRINGTON & SMITH, PC 4 RESEARCH DRIVE, Suite 202 SHELTON, CT 06484-6212				
EXAMINER				
LEE, ANDREW CHUNG CHEUNG				
ART UNIT		PAPER NUMBER		
2476				
MAIL DATE		DELIVERY MODE		
12/08/2009		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/531,491

Applicant(s)

WARIS, HEIKKI

Examiner

Andrew C. Lee

Art Unit

2476

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 August 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 and 22-36 is/are pending in the application.
- 4a) Of the above claim(s) 19-21 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18 and 22-36 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB-08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 19 – 21 have been canceled.

Claims 1 – 18, 22 – 36 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 29, 32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Regarding claim 29, the possessive pronoun "its" in the newly amended claim subject matter "wherein the mobile enters a security association for the second gateway into its security association database" is very ambiguous. One of ordinary skill in the art has difficult time to understand what/which claim subject matter "its" refers to. Clarification and appropriate action are required. Claim 32 has the same deficiencies as claim 29.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1 – 13, 15, 17 – 28, 30, 31, 33, 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kakemizu et al. (US 20020018456 A1) and Lee et al. (US 20020085517 A1) in view of Van Oorschot (US 6370249 B1).

Regarding claim 1, Kakemizu et al. disclose a network (*Fig. 1, Fig. 2, Fig 4*) comprising: an internal secured portion (*"VPN of IP sec." interpreted as internal secured portion; Fig. 2, para. [0017], Fig. 25, para. [0113]*), except comprising a first virtual private network certificate authority and a second virtual private network certificate authority; an external portion (*"public IP network" interpreted as an external portion; Fig. 2, para. [0017], Fig. 25, para. [0113]*); at least one mobile node in the external portion element (*"MN 1" interpreted as at least one mobile node in the external portion; para. [0017]*); at least a first gateway (*Fig. 2, "element 21 VPNGW(FA)" interpreted as the first gateway; para. [0017]*) except associated with the first virtual private network certificate authority; and at least a second gateway (*"element 31 VPNGW(HA)" interpreted as a second gateway*) except associated with the second virtual private network certificate authority, where the internal secured portion connects via the first gateway and the second gateway to the external portion (*Fig. 2, Fig. 4, VPN of IP sec." interpreted as internal secured portion, "element 21 VPNGW(FA)" interpreted as the first gateway, "element 31 VPNGW(HA)" interpreted as a second gateway; Fig. 2, para [0017], Fig. 25, para [0113]*), and the network is configured to change the gateway, which the mobile node uses to communicate with the internal secured portion, from the first gateway to the second gateway in response to movement of

Art Unit: 2476

the mobile node (*Fig. 25, Fig. 26, paras.[0113], [0119] – [0121]*) except via the first and the second virtual private network certificate authorities. Kakemizu et al. also disclose care-of-address ("*care-of-address*"; *para. [0100]*).

Kakemizu et al. do not disclose explicitly in response to a receipt from the mobile node of a new care- of-address that is different from a first care-of-address.

Lee et al. in the same field of endeavor teach in response to a receipt from the mobile node of a new care- of-address that is different from a first care-of-address ("*using a newly allocated COA*"; *para. [0043], Fig. 6, para. [0095]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. to include the features of in response to a receipt from the mobile node of a new care- of-address that is different from a first care-of-address as taught by Lee et al. One of ordinary skill in the art would be motivated to do so for providing a gatekeeper supporting a handoff in an IP telephony system (*as suggested by Lee et al., see para. [0036]*).

The combined system of Kakemizu et al. and Lee et al. does not disclose explicitly a first virtual private network certificate authority and a second virtual private network certificate authority; at least a first gateway associated with the first virtual private network certificate authority; and at least a second gateway associated with the second virtual private network certificate authority; the first gateway to the second gateway via the first and the second virtual private network certificate authorities.

Van Oorschot in the same field of endeavor teaches a first virtual private network certificate authority and a second virtual private network certificate authority (*Fig. 1, Fig. 2, certification authority 34 in locate 18 interpreted as first virtual private network certificate authority, and certification authority 46 in locate 20 interpreted as a second virtual private network certificate authority; col. 4, lines 36 – 48*); at least a first gateway associated with the first virtual private network certificate authority (*directory 36 interpreted as a first gateway; Fig. 1, col. 4, lines 36 - 48*); and at least a second gateway associated with the second virtual private network certificate authority (*directory 48 interpreted as a second gateway; Fig. 1, col. 4, lines 36 - 48*); the first gateway to the second gateway via the first and the second virtual private network certificate authorities (*col. 4, lines 36 – 48, Fig. 2, col. 7, lines 7 – 34*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of a first virtual private network certificate authority and a second virtual private network certificate authority; at least a first gateway associated with the first virtual private network certificate authority; and at least a second gateway associated with the second virtual private network certificate authority; the first gateway to the second gateway via the first and the second virtual private network certificate authorities as taught by Van Oorschot. One of ordinary skill in the art would be motivated to do so for providing a method and apparatus for public key management that allows a client to obtain multiple trusted public keys of various certificate authorities on-line, where the ability to change a

Art Unit: 2476

client's trusted public keys is a privilege granted by the system (rather than the end-user) and the efficiency of the secure communication system does not suffer (as suggested by Van Oorschot, see col. 2, lines 50 – 56).

Regarding claim 2, Kakemizu et al. disclose a network as claimed further configured to transfer context information usable by the at least first gateway in communications with the mobile node, to the second gateway (*Fig. 25, paragraphs [0114], [0115]*).

Regarding claim 3, Kakemizu et al. disclose a network as claimed wherein the context information includes an identifier of the mobile node (*"care-of-address" interpreted as context information includes an identifier of the mobile node; paras [0004], [0100]*).

Regarding claim 4, Kakemizu et al. disclose a network as claimed wherein the identifier is a home address of the mobile node (*"home address"; paras [0004], [0100]*).

Regarding claim 5, Kakemizu et al. disclose a network as claimed wherein the context information includes material for defining secure communication means by which information is transferable securely between the mobile node in the external portion of the network and the internal secured portion of the network, via the second gateway (*paras [0017], [0024], Fig. 2, Fig. 27*).

Regarding claim 6, Kakemizu et al. disclose a network as claimed wherein the secure communication means is a security association pair between the second gateway and the mobile node (*Fig. 27, "position registration request*

message (HAR), and "position registration response (HAA)" interpreted as secure communication means is a security association pair; paras [0128], [0129].

Regarding claim 7, Kakemizu et al. disclose a network as claimed wherein the context information is transferred from a location that is physically separate from the first gateway ("*element 23 AAAF*"; *Fig. 27, paras [0127], [0129]*).

Regarding claim 8, Kakemizu et al. disclose a network as claimed further configured to transfer information to the mobile node for enabling communications between the mobile node and the second gateway (*Fig. 27, para [0129]*).

Regarding claim 9, Kakemizu et al. disclose a network as claimed wherein the information transferred to the mobile node enables secure communication means by which information is transferable securely between the mobile node in the external portion of the network and the internal secured portion of the network, via the second gateway ("*elements "Reg Req 1, and Reg Rep 8 and authentication request message , AMR"* interpreted as the information transferred to the mobile node enables secure communication means; *Fig. 27, paras [0127]-[0129]*).

Regarding claim 10, Kakemizu et al. disclose a network as claimed wherein the secure communication means is a security association pair between the mobile node and the second gateway (*Fig. 27, "position registration request message (HAR), and "position registration response (HAA)" interpreted as secure communication means is a security association pair; paras [0128], [0129]*).

Regarding claim 11, Kakemizu et al. disclose a network as claimed wherein the information transferred to the mobile node comprises an address of the second gateway (*Fig. 27, para. [0128]*).

Regarding claim 12, Kakemizu et al. disclose a network as claimed wherein the information transferred to the mobile node is transferred between the first gateway and the mobile node using an existing security association between the mobile node and the first gateway (*elements "Reg Req 1, and Reg Rep 8 and authentication request message , AMR" interpreted as the information transferred to the mobile node is transferred between the first gateway and the mobile node; Fig. 27, paras [0127]-[0129]*).

Regarding claims 13, 15, Kakemizu et al. disclose a network as claimed wherein the second gateway comprises one or more databases which are updated to enable the internal secured portion of the network and the mobile node in the external portion of the network to communicate via the second gateway (*"element 34 VPN database"; Fig. 27, paras [0128], [0129]*).

Regarding claim 17, Kakemizu et al. disclose a network as claimed further configured to detection means for detecting a present location of the mobile node and change gateway through which the mobile node communicates with the internal secured portion of the network, from the first gateway to a better gateway (*element 33 AAAH" interpreted as the location detection means; Fig. 25, Fig.26, paras [0119]-[0121]*).

Regarding claim 18, Kakemizu et al. disclose a network as claimed wherein the better gateway is better because it is either closer to the mobile node or it is optimal for routing existing sessions (*Fig. 13, paras [0080], [0081]*).

Regarding claim 22, Kakemizu et al. disclose a network as claimed further configured to detect a present location via a location detection means that is separate from the first gateway (*"element 33 AAAH" interpreted as configured to detect a present location from a source that is separate from the first gateway (VPHGW(HA) interpreted as first gateway); Fig. 25, Fig.26, paras [0119]-[0121]*).

Regarding claim 23, Kakemizu et al. disclose a network as claimed further configured to transfer information via transfer means physically separate from the first gateway and wherein the transfer means and the location detection means are housed together (*Fig. 6, paras [0071], [0072]*).

Regarding claim 24, Kakemizu et al. disclose a network as claimed wherein the first gateway and the second gateway are in distinct physically separated segments of the network (*VPNGW(FA) interpreted as first gateway which is located at roaming-contracted ISP network, and VPNGW(HA) interpreted as second gateway which is located at HOME ISP; Fig. 25, Fig. 26*).

Regarding claim 25, Kakemizu et al. disclose a network as claimed wherein the mobile node communicates with the internal secured portion of the network via the first gateway and also via the second gateway simultaneously for a transition period, before communicating via the second gateway only (*Fig. 26, paras [0120]-[0121]*).

Regarding claim 26, Kakemizu et al. disclose a network as claimed wherein the mobile node is involved in a session with a correspondent node (*para [0128]*).

Regarding claim 27, Kakemizu et al. disclose a network as claimed wherein the correspondent node is located in the internal secured portion of the network and the mobile node is located in the external portion of the network (*"CN" interpreted as correspondent node is located in the internal portion of the network; "MN 1" interpreted as the mobile node is located in the external portion of the network; Fig. 2, Fig. 26*).

Regarding claim 28, Kakemizu et al. disclose a method comprising: determining when a first serving gateway except associated with a first virtual private network certificate authority, through which a mobile node communicates from an external portion of a network with an internal secured portion of the network, is suboptimal (*Fig. 13, paras [0080], [0081]*); identifying a second gateway (*"reads the address of the VPNGW"; paras [0080], [0081]*), except associated with a second virtual private network certificate authority; and in response to the mobile node moving (*Fig. 26, paras. [0119]*), and transferring the point the gateway through which the mobile node communicates with the internal portion of the network from the first serving gateway to the second gateway (*Fig. 26, paras. [0119] – [0121]*), except sending a new care-of-address that is different from a first care-of-address to the first serving gateway, and via the first and second virtual private network certificate authorities.

Kakemizu et al. do not disclose explicitly sending a new care-of-address that is different from a first care-of-address to the first serving gateway.

Lee et al. in the same field of endeavor teach sending a new care-of-address that is different from a first care-of-address to the first serving gateway ("*using a newly allocated COA*"; para. [0043] "; para. [0043], Fig. 6, para. [0095]).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. to include the features of sending a new care-of-address that is different from a first care-of-address to the first serving gateway as taught by Lee et al. One of ordinary skill in the art would be motivated to do so for providing a gatekeeper supporting a handoff in an IP telephony system (*as suggested by Lee et al., see para. [0036]*).

The combined system of Kakemizu et al. and Lee et al. does not disclose explicitly first serving gateway associated with a first virtual private network certificate authority ; a second gateway associated with a second virtual private network certificate authority; from the first serving gateway to the second gateway via the first and second virtual private network certificate authorities.

Van Oorschot in the same field of endeavor teaches first serving gateway associated with a first virtual private network certificate authority (*directory 36 interpreted as a first gateway; Fig. 1, col. 4, lines 36 – 48; Fig. 1, Fig. 2, certification authority 34 in locate 18 interpreted as first virtual private network certificate authority*); and a second gateway associated with a second virtual private network certificate authority (*directory 48 interpreted as a second gateway; Fig. 1, col. 4, lines 36 – 48; certification authority 46 in locate 20 interpreted as a*

Art Unit: 2476

second virtual private network certificate authority; col. 4, lines 36 – 48); from the first serving gateway to the second gateway via the first and second virtual private network certificate authorities (col. 4, lines 36 – 48, Fig. 2, col. 7, lines 7 – 34).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of first serving gateway associated with a first virtual private network certificate authority ; a second gateway associated with a second virtual private network certificate authority; from the first serving gateway to the second gateway via the first and second virtual private network certificate authorities as taught by Van Oorschot. One of ordinary skill in the art would be motivated to do so for providing a method and apparatus for public key management that allows a client to obtain multiple trusted public keys of various certificate authorities on-line, where the ability to change a client's trusted public keys is a privilege granted by the system (rather than the end-user) and the efficiency of the secure communication system does not suffer *(as suggested by Van Oorschot, see col. 2, lines 50 – 56).*

Regarding claim 30, Kakemizu et al. disclose a mobile node as claimed further comprising means for using a first secure communication means by which information is transferable securely between the internal portion of the network and the mobile node via the first gateway, to receive the identifier of the second gateway *(elements “Reg Req 1, and Reg Rep 8 and authentication request message , AMR” interpreted as the information transferred to the mobile*

node is transferred between the first gateway and the mobile node; Fig. 27, paragraphs [0127]-[0129]);

Regarding claim 31, Kakemizu et al. discloses a mobile node as claimed further comprising means for using a second secure communication means to transfer information securely between the internal portion of the network and the mobile node via the second gateway (*Fig. 27, "position registration request message (HAR), and "position registration response (HAA)" interpreted as means for using a second secure communication means; paragraphs [0128], [0129]*).

Regarding claims 33, 34, Kakemizu et al. disclose a method and apparatus comprising and an apparatus configured to (*Fig. 1, Fig. 2, Fig. 4*): updating a location database in order to change an identification of a gateway that the mobile node uses to communicate from an external portion of the network to an internal secured portion of the network (*paras. [0113], [0119]-[0121]*), except receiving a new care-of-address that is different from a first care-of-address from a mobile node that has moved in a network, and the first gateway is associated with a first virtual private network certificate authority in the internal secured portion and the second gateway is associated with a second virtual private network certificate authority in the internal secured portion, wherein context information for the mobile node is transferred from the first virtual private network certificate authority to the second virtual private network certificate authority.

Kakemizu et al. do not disclose explicitly receiving a new care-of-address that is different from a first care-of-address from a mobile node that has moved in a network.

Lee et al. in the same field of endeavor teach receiving a new care-of-address that is different from a first care-of-address from a mobile node that has moved in a network (*"using a newly allocated COA"; para. [0043], para. [0043], Fig. 6, para. [0095]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. to include the features of receiving a new care-of-address that is different from a first care-of-address from a mobile node that has moved in a network as taught by Lee et al. One of ordinary skill in the art would be motivated to do so for providing a gatekeeper supporting a handoff in an IP telephony system (*as suggested by Lee et al., see para. [0036]*).

The combined system of Kakemizu et al. and Lee et al. teaches mobile node and all the limitations as addressed above, but does not disclose explicitly the first gateway is associated with a first virtual private network certificate authority in the internal secured portion and the second gateway is associated with a second virtual private network certificate authority in the internal secured portion, wherein context information for the mobile node is transferred from the first virtual private network certificate authority to the second virtual private network certificate authority.

Van Oorschot in the same field of endeavor teaches the first gateway is associated with a first virtual private network certificate authority in the internal secured portion (*directory 36 interpreted as a first gateway; Fig. 1, col. 4, lines 36 – 48; Fig. 1, Fig. 2, certification authority 34 in locate 18 interpreted as first virtual*

Art Unit: 2476

private network certificate authority) and the second gateway is associated with a second virtual private network certificate authority in the internal secured portion (directory 48 interpreted as a second gateway; Fig. 1, col. 4, lines 36 – 48; certification authority 46 in locate 20 interpreted as a second virtual private network certificate authority; col. 4, lines 36 – 48), wherein context information for the mobile node is transferred from the first virtual private network certificate authority to the second virtual private network certificate authority (col. 4, lines 36 – 48, Fig. 2, col. 7, lines 7 – 34).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of the first gateway is associated with a first virtual private network certificate authority in the internal secured portion and the second gateway is associated with a second virtual private network certificate authority in the internal secured portion, wherein context information for the mobile node is transferred from the first virtual private network certificate authority to the second virtual private network certificate authority as taught by Van Oorschot. One of ordinary skill in the art would be motivated to do so for providing a method and apparatus for public key management that allows a client to obtain multiple trusted public keys of various certificate authorities on-line, where the ability to change a client's trusted public keys is a privilege granted by the system (rather than the end-user) and the efficiency of the secure communication system does not suffer (as suggested by Van Oorschot, see col. 2, lines 50 – 56).

Regarding claimed 35, Kakemizu et al. disclose the network is a virtual private network ("*VPN*"; *Abstract, Fig. 1, para. [0010], Fig. 4, para. [0063]*)

5. Claims 14, 16, 29, 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kakemizu et al. (US 20020018456 A1), Lee et al. (US 20020085517 A1) and Van Oorschot (US 6370249 B1) as applied to claims 1, 13, 15 above, and further in view of Shapira et al. (US 7107464 B2).

Regarding claims 14, 16, Kakemizu et al. disclose a network as claimed wherein the second gateway comprises one or more databases ("*element 34 VPN database*"; *Fig. 27, paras [0128], [0129]*).

Kakemizu et al. and Lee et al. do not disclose explicitly wherein the one or more databases are a security policy database and a security association database.

Shapira et al. in the same field of endeavor teach wherein the one or more databases are a security policy database and a security association database ("*a security association database (SAD)*"; *col. 6, lines 47 – 54, "Security Policy Database (SPD)*"; *col. 14, lines 39 – 48*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of wherein the one or more databases are a Security Policy Database and a Security Association Database as taught by Shapira et al. One of ordinary skill in the art would be motivated to do so for providing a mechanism for implementing virtual private networks (VPNs) incorporating a security association

Art Unit: 2476

database and associated processor (*as suggested by Shapira et al., see col. 1, lines 8 – 11*).

Regarding claim 29, Kakemizu et al. disclose a mobile node (*Fig. 1, Fig. 2, Fig. 4*) comprising: means for receiving, via a first secure communication means, an identifier of a second gateway (*Fig. 27, para. [0128]*); and means for changing from communicating with an internal secured portion of the network through the first gateway to communicating via the second gateway (*Fig. 27, paras. [0128],[0129]*), where the mobile node enters a security association for the second gateway (*Fig. 29, paras. [0130], [0140]*) except into its security association database, and in response to moving and sending a new care-of-address that is different from a first care-of- address to the first gateway.

Kakemizu et al. do not disclose explicitly in response to moving and sending a new care-of-address that is different from a first care-of- address to the first gateway.

Lee et al. in the same field of endeavor teach in response to moving and sending a new care-of-address that is different from a first care-of- address to the first gateway (*"using a newly allocated COA"; para. [0043], para. [0043], Fig. 6, para. [0095]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. to include the features of in response to moving and sending a new care-of-address that is different from a first care-of- address to the first gateway as taught by Lee et al. One of ordinary skill in the art would be motivated to do so for providing a

Art Unit: 2476

gatekeeper supporting a handoff in an IP telephony system (*as suggested by Lee et al., see para. [0036]*).

The combined system of Kakemizu et al. and Lee et al. does not disclose explicitly a security association database.

Shapira et al. in the same field of endeavor teach a security association database (*"a security association database (SAD)"; col. 6, lines 47 – 54*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of a Security Association Database as taught by Shapira et al. One of ordinary skill in the art would be motivated to do so for providing a mechanism for implementing virtual private networks (VPNs) incorporating a security association database and associated processor (*as suggested by Shapira et al., see col. 1, lines 8 – 11*).

Regarding claim 32, Kakemizu et al. disclose a method comprising: moving by a mobile node in an external portion of a network, where the network comprises an internal secured portion, the external portion, at least a first gateway, and at least a second gateway; obtaining a location identifier (*Fig. 27, paragraphs [0128]-[0129]*), wherein the mobile node enters a security association for the second gateway (*Fig. 29, paras. [0130], [0140]*). Kakemizu et al. also disclose where the location identifier comprises a care-of-address (*"care-of-address"; para. [0100]*).

Kakemizu et al. do not disclose explicitly a new care-of-address different from a first care-of-address; sending the new care-of-address to the first gateway;

Art Unit: 2476

and in response to receiving an acknowledgement from the second gateway, communicating via the second gateway, and security association database.

Lee et al. in the same field of endeavor teach a new care-of-address different from a first care-of-address; sending the new care-of-address to the first gateway; and in response to receiving an acknowledgement from the second gateway, communicating via the second gateway (*"using a newly allocated COA"; para. [0043], para. [0043], Fig. 6, para. [0095]*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. to include the features of a new care-of-address different from a first care-of-address; sending the new care-of-address to the first gateway; and in response to receiving an acknowledgement from the second gateway, communicating via the second gateway as taught by Lee et al. One of ordinary skill in the art would be motivated to do so for providing a gatekeeper supporting a handoff in an IP telephony system (*as suggested by Lee et al., see para. [0036]*).

The combined system of Kakemizu et al. and Lee et al. does not disclose explicitly a security association database.

Shapira et al. in the same field of endeavor teach a security association database (*"a security association database (SAD)"; col. 6, lines 47 – 54*).

At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Kakemizu et al. and Lee et al. to include the features of a Security Association Database as taught by Shapira et al. One of ordinary skill in the art would be motivated to do so for providing a

Art Unit: 2476

mechanism for implementing virtual private networks (VPNs) incorporating a security association database and associated processor (*as suggested by Shapira et al., see col. 1, lines 8 – 11*).

6. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot (US 6370249 A1) in view of Kakemizu et al. (US 20020018456 A1).

Regarding claim 36, Van Oorschot discloses a virtual private network certificate authority ("*certification authority*"; *Abstract, Fig. 1*), comprising: means for forming first and second security associations between and with a node and the virtual private network certificate authority (*Fig. 1, Fig. 2, col. 14, lines 17 – 28*), except a mobile node; Van Oorschot also discloses means for updating a location database (*col. 14, lines 33 – 40*); and Van Oorschot further discloses means for forming first and second security associations between and with a gateway node and the virtual private network certificate authority (*Fig. 1, Fig. 2, col. 4, lines 36 – 48*), wherein the first and second security associations between and with the node and the virtual private network certificate authority and between and with the gateway node and the virtual private network certificate authority are encapsulating security payload security associations ("*security-related operation*"; *Fig. 2, col. 7, lines 7 – 34; Fig. 4, col. 9, lines 9 – 19, 45 – 65*).

Van Oorschot does not disclose a mobile node. Kakemizu et al. in the same field of endeavor teach a mobile node (*Fig. 4, Fig. 13, paras [0080], [0081]*). At time the invention was made it would have been obvious to a person of ordinary skill in the art to modify the teachings of Van Oorschot to include the

Art Unit: 2476

features of a mobile node as taught by Kakemizu et al. One of ordinary skill in the art would be motivated to do so for providing a VPN setting service that enables the communications in the mobile IP to be carried out by using a safe communication path (*as suggested by Kakemizu et al., see para. [0012]*).

Response to Arguments

7. Applicant's arguments filed on 8/07/2009 with respect to claims 1 – 9, 22 – 36 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a) Jing et al. (US 7298847 B2).
- b) Xu et al. (US 6738362 B1).
- c) Amin et al. (US 6714987 B1).

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will

Art Unit: 2476

the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew C. Lee whose telephone number is (571)272-3131. The examiner can normally be reached on Monday through Friday from 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew C Lee/
Examiner, Art Unit 2476
<1Qy10:12/02/2009>
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2476